02-07

FORM PTO-1390 (REV. 5-93)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER 2643/0G629 PCT
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)		09/485352
INTERNATIONAL APPLICATION NO. PCT/DE98/01943	INTERNATIONAL FILING DATE 13 July 1998	PRIORITY DATE CLAIMED August 4, 1997

TITLE OF INVENTION

METHOD AND DEVICE FOR CUSTOMER PERSONALIZATION OF GSM CHIPS

APPLICANT(S) FOR DO/EO/US

Michael DUPRÉ

Applicant herewith submits to the United States Designated/Elected office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.

2. [] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S. C. 371.

3. [] This is an express request to begin national examination procedures (35 U.S.C. 371 (f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S. C. 371 (b) and PCT Articles 22 and 39 (1).

4. [X] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [X] A copy of the International Application as filed (35 U.S. C. 371 (c) (2))
   a. [] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [X] has been transmitted by the International Bureau
   c. [] is not required, as the application was filed in the Untied States Receiving Office (RO/US)

6. [X] A translation of the International Application into English (35 U.S. C. 371 (c)2)).

7. [] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. [] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [] have been transmitted by the International Bureau.
   c. [] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [] have not been made and will not be made.

8. [] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c) (3)).

9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4) (unsigned)).

10. [] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.79 and 1.98.

12. [] An assignment document for recording. A **separate** cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. [X] A FIRST preliminary amendment.
    [] A SECOND or SUBSEQUENT preliminary amendment.

14. [] A substitute specification.

15. [] A change of power of attorney an/or address letter.

16. [X] Other items or information: Substitute Pages, Translation of Substitute Pages.

EXPRESS MAIL CERTIFICATE
Date 2/4/2000 Label No. EL503340143
I hereby certify that, on the date indicated above I deposited this paper or fee with the U.S. Postal Service & that it was addressed for delivery to the Commissioner of Patents & Trademarks, Washington D.C. 20231 by "Express Mail Post Office to Addressee" service.
D B Peck
Name (Print)
Signature

U.S. APPLICATION NO. (if known, see 37 C.F.R 1.50 09/485352	INTERNATIONAL APPLICATION NO.: PCT/DE98/01943	Attorney's Docket Number 2643/0G629

		CALCULATIONS	PTO USE ONLY
17. [X] The following fees are submitted:			
Basic National Fee (37 CFR 1.492 (a)(1)-(5)): Search Report has been prepared by the EPO [X] or JPO []	$840.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482)	$670.00		
No international preliminary examination fee paid to USPTO(37 CFR 4.482) but international search fee paid to USPTO (37 CFR 1.445 (a) (2)...	$760.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO.........	$970.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)...........	$96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =		$840.00	
Surcharge of $130.00 for furnishing the oath or declaration later than []20 []30 months from the earliest claimed priority date (37 CFR 1.492(e)).		$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	9	0	0 X $18.00	$0	
Independent Claims	2	0	0 X $78.00	$0	
Multiple dependent claims(s) (if applicable)		+260		$	

TOTAL OF ABOVE CALCULATIONS =	$840.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).	$	
SUBTOTAL =	$840.00	
Processing fee of **$130.00** for furnishing the English translation later the [] 20 [] 39 months from the earliest claimed priority date (37 CFR 1.492(f)). +	$	
TOTAL NATIONAL FEE =	$840.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). the assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$0.00	
TOTAL FEES ENCLOSED =	$840.00	
	Amount to be refunded	$
	charged	$

a. [X] A check in the amount of $840.00 to cover the above fees is enclosed.

b. [] Please charge my Deposit Account No.04-0100 in the amount of $ to cover the above fees.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 04-0100. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO
Christa Hildebrand, Esq.
Darby & Darby P.C.
805 Third Avenue
New York, New York 10022-7513

SIGNATURE Christa Hildebrand

NAME Christa Hildebrand

REGISTRATION NO. 34,953

3-15-00

PCT

EXPRESS MAIL CERTIFICATE

Date 3/14/00 Label No. EL503340792 US

I hereby certify that, on the date indicated above I deposited this paper or fee with the U.S. Postal Service & that it was addressed for delivery to the Commissioner of Patents & Trademarks, Washington D.C. 20231 by "Express Mail Post Office to Addressee" service.

D Beck Name (Print)

Beck Signature

CERTIFICATE OF MAILING

I hereby certify that this paper and every
paper referred to therein as being enclosed
is being deposited with the U.S. Postal Service
as first class mail, postage prepaid, in
an envelope addressed to: Commissioner of
Patents & Trademarks, Washington, DC 20231,

on ______________________(Date of Deposit)

________ ____________________
Date Name

File No.: 2643/0G629

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Michael DUPRÉ

Serial No.:	09/485,352	Group Art Unit:	Not Assigned
Filed:	February 4, 2000	Examiner:	Not Assigned
For:	**METHOD AND DEVICE FOR CUSTOMER PERSONALIZATION OF GSM CHIPS**		

Hon. Commissioner of
Patents and Trademarks
Washington, DC 20231

Sir:

COMPLETION OF PATENT APPLICATION

The following items are submitted herewith in completion of the above-identified patent application:

1. Declaration, petition and power of attorney

2. Check in the amount of $,170.00 $40.00 recording)
(See attached Fee Computation Sheet)

3. [] Formal drawings, sheets (Figs.)
[] Informal drawings, sheets (Figs.)

4. [X] Assignment for recording to:

DeTeMobil Deutsche Telekom MobilNet GmbH
Landgrabenweg 151
D-53227 Bonn, GERMANY

5. [] Verified statement claiming small entity status.
PARTIAL REFUND of all fees paid within last 2 months is REQUESTED.

Priority is claimed for this application, corresponding application/s having been filed as follows:

Country:	Germany
Number:	197 33662.0
Date:	August 4, 1997

The priority documents [] are enclosed
[] will follow.

The Patent Office is authorized to charge any deficiency up to $300.00 in the above fees, and to credit any excess, to our Deposit Account No. 4-0100.

Dated: March 14, 2000

Respectfully submitted,

Christa Hildebrand

Christa Hildebrand
Reg. No. 34,953
Attorney for Applicant(s)

DARBY & DARBY P.C.
805 Third Avenue
New York, NY 10022
212-527-7700
(D&DForms/PTO-5)

File No.: 1613/0G321

PATENT FEE COMPUTATION SHEET

	No. of Claims Presented	Extra Claims Previously Paid For	Number of Extra Claims	Rate	
Basic Fee					$
Design Application					$
Plant Application					$
Total Claims	13- 20	- =	x $18.00		$
Independent Claims	1 - 3	- =	x $78.00		$
Multiple Dependent Claims		x- if so, add	$260.00		$
Surcharge for late submission of filing fee and/or declaration ($130.00)					$130.00
SUBTOTAL					$130.00
[] Small Entity REDUCTION (Half of Subtotal)					$
Fee for recordation of assignment ($40.00)					$40.00
Charge for filing non-English language application ($130.00)					$
TOTAL					$170.00

EXPRESS MAIL CERTIFICATE

Date 2/4/2000 Label No. EL503340143

I hereby certify that, on the date indicated above I deposited this paper or fee with the U.S. Postal Service and that it was addressed for delivery to the Commissioner of Patents & Trademarks, Washington, DC 20231 by "Express Mail Post Office to Addressee" service.

D B Peck

Name (Print)

D Peck

Signature

PLEASE CHARGE ANY DEFICIENCY UP TO $300.00 OR CREDIT ANY EXCESS IN FUTURE FEES DUE WITH RESPECT TO THIS APPLICATION TO OUR DEPOSIT ACCOUNT NO. 04-0100

DARBY & DARBY P.C.
805 Third Avenue
New York, New York 10022
212-527-7700

File No: 2643/0G629

In Re Application of:

DUPRÉ, Michael

For: **METHOD AND DEVICE FOR CUSTOMER PERSONALIZATION OF GSM CHIPS**

PRELIMINARY AMENDMENT

Hon. Commissioner of
Patents and Trademarks
Washington, DC 20231

Sir:

Please preliminarily amend the above identified application as follows:

IN THE CLAIMS:

Please cancel claims 1-13 and enter new claims 14 - 22 as follows:

14. A method for personalizing GSM chips having a memory range in which at least one subscriber identification number IMSI and a card number ICCID are stored, and wherein for personalizing the chip an additional secret key Ki and, optionally, additional data are stored, wherein at the manufacturer for pre-personalizing the chip, at least initial card-specific data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK are stored, comprising the steps of

a) performing the personalization of the chip when the subscriber logs on to the subscriber network for the first time;

b) obtaining the ICCID and the IMSI from a number pool, the chip itself derives an initial key Ki_1 from a key K1 which is known and entered into the chip, while PIN and PUK are set to a default value;

c) making an entry in the authentication center (AC) and the home location register (HLR) as soon as a subscriber has entered into a contract with the network operator;

d) deriving the authentication center (AC) the initial first key Ki_1;

e) setting the conditions of the network so that during logon to the network, a connection is established from the chip to the security center of the network operator (SC);

f) routing the connection from the chip to the SC during the first logon;

g) negotiating a new second secret key Ki_2 and, optionally, a PUK with the chip or generated in the security center (SC) and transmitted to the chip;

h) disabling the conditions of step e).

15. The method according to claim 14, wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the AC before the contract is established.

16. The method according to claim 14, further comprising the step of employing a Diffie-Hellman method to negotiate the second secret key Ki_2.

17. The method according to claim 16, wherein the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag).

18. The method according to claim 17, wherein , when the initial key Ki_1 is entered into the authentication center (AC) for the first time, the hotlining flag is also set in the home location register (HLR).

19. A chip having stored in the memory range at least one subscriber identification number IMSI and a card number ICCID as well as for the purpose of personalization an additional secret key Ki and, optionally, additional data, wherein for pre-personalizing the chip there are further stored initial card-related data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK, wherein the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a key.

20. The chip according to claim 19, wherein the chip includes means for receiving data from the security center (SC) and means for writing these data to a memory and, optionally, reading these data from the memory, changing these data and/or transmitting these data to the security center (SC).

21. The chip according to claim 20, wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC).

22. The chip according to claim 21, wherein the chip includes a dialing number which is fixedly programmed by the manufacturer (fixed dialing).

IN THE SPECIFICATION:

On page 1, line 3, delete "Description" and insert instead

--**BACKGROUND OF THE INVENTION**

1. Field of the Invention--;

On page 2, line 19, please insert:

--**2. Description of the Related Art**

EP-A-562 890 discloses a mobile communication network having the capability for remotely updating a so-called subscriber identification module (SIM) in mobile stations. The SIM stores data for controlling the mobile stations and for access to the services of the mobile radio network. The data stored in the SIM can be changed, i.e., updated, over the radio air interface. However, a method for personalizing a SIM over the air interface is not described.

WO-A-97/14258 also describes a method and a device for programming a mobile station via an air interface. Optionally, programs stored in the mobile station are here replaced or additional data are transmitted via the air interface. The method described herein also permits an initial activation of the mobile station via the air interface, but not a personalization of a subscriber identification module.

WO-A-93/07697 relates to a method for personalizing an active so-called SIM card. The SIM card is here completely personalized in an authorized terminal equipment which is connected via an encrypted communication line with a the central computer of the mobile radio network. However, a personalization of the chip card when the subscriber first logs on to the mobile radio network, is also neither taught nor suggested by this reference.- -

Page 2, please delete line 24-27 and

Page 3 delete entirely and insert instead

- - **<u>SUMMARY OF THE INVENTION</u>**

To solve the object, the invention propose that the personalization of the chip is performed when the subscriber logs on to the subscriber network for the first time, wherein the following process steps are carried out in that in a first process step, the chip manufacturer obtains the ICCID and the IMSI from a number pool, the chip itself derives an initial key Ki_1 from a key K1 which is known to and entered into the chip by the chip manufacturer, while PIN and PUK are set to a default value, in a second process step, an entry is made in the authentication center (AC) and the home location register (HLR) as soon as a subscriber has entered into a contract with the network operator, in a third process step, the authentication center (AC) also derives the initial first key Ki_1, in a fourth process step, the network sets the conditions so that during logon to the network, a connection is established from the chip to the security center of the network operator (SC), in a fifth process step, the connection is routed from the chip to the SC during the first logon, in a sixth process step, a new second secret key Ki_2 and, optionally, a PUK is negotiated with the chip or generated in the security center (SC) and transmitted to the chip, in a seventh process step, the conditions of the fourth process step are disabled again.

Further, a chip is provided wherein in the memory range of the chip there are stored at least one subscriber identification number IMSI and a card number ICCID as well as for the purpose of personalization an additional secret key Ki and, optionally, additional data, wherein for pre-personalizing the chip there are further stored initial card-related data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK, characterized in that the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a key.

The technical teachings according to the invention attains the following advantages: Elimination of a central personalization at the network operator; Issuance of a large number of GSM chips without producing a static load at the network operator; Reuse of "used" GSM chips; Regular change of the secret key Ki while used by the customer.

With the proposed method, the device manufacturer/chip manufacturer applies initial data associated with the card to the chip, which could be referred to as pre-personalization. The network operator himself performs the actual personalization at a later time and only for those customers who enter into a contract with the network operator.

The pre-personalization does not yet produce a static load at the network operator. The method therefore makes it possible to distribute "millions" of GSM chips, for example in each and every automobile, in each laptop computer or in each alarm system, and to subsequently "activate" only the chips of those customers who enter into a contract.

It is also possible to reuse cards if a customer terminates his contract (for example, if he sells his automobile).

In particular, in the case of the network operator D1, the dealer could release returned cards again for another customer. The network operator therefore eliminates the personalization of cards in the terminal equipment replacement business.

On page 9, on line 11, please insert:

-- **<u>BRIEF DESCRIPTION OF THE DRAWINGS</u>** --;

On page 9, line 20, please insert:

<u>--DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENTS</u> --;

On page 15, delete "SUMMARY" and insert --ABSTRACT- -;

REMARKS

This Preliminary Amendment has been made to add/replace the substitute pages from the PCT International application into the national phase prosecution and to prosecute the claims that were submitted as replacement claims. Such claims have been rewritten to conform to the US prosecution standards. No new matter was added.

An early and favorable action on the merits is respectfully requested.

Respectfully submitted,

Christa Hildebrand

Christa Hildebrand, Esq.
Registration No. 34,953
Attorney for Applicants

Darby & Darby, P.C.
805 Third Avenue
New York, New York 10022
(212) 527-7700

M \2643\0G629\CH7993 WPD

Method and device for customer personalization of GSM chips

Description

A method is proposed for customer personalization of GSM chips which assumes that the chip at the time of the personalization is located in the terminal equipment of the customer.
According to the present state of the art, the network operators presently implement the GSM chip in a GSM card which is inserted in the terminal equipment. The chip may also be permanently integrated in the terminal equipment, for example, on a plug-in card of a computer. It is not important for the present method if a GSM card or a terminal with an integrated chip is employed. A "chip" in the broadest sense is understood to be an EPROM, an EEPROM, as well as an "intelligent" microprocessor.

Regardless of a particular embodiment, the following discussion will use the term "chip" and "chip manufacturer."

With centralized personalization used until now, the chip receives, aside from other data, a card number (ICCID), a subscriber identification number (IMSI) as well as several secret numbers. While the chip manufacturer can easily apply the data ICCID and IMSI to the chip, the network operator likes to keep control over the secret numbers, in particular over the key Ki, which should be known only to the card and the network.

With the present centralized personalization, the network operator receives from the card manufacturer unmarked cards and subsequently writes the final secret key.

Replacement sheet 2

Accordingly, this key is only known to two localities, namely the chip itself and the network operator.

Disadvantageously, an extraordinarily large static load is produced in the computer center of the network operator. A generator generates a large number of keys which are then applied to the respective cards. The key generated for each card is then simultaneously transmitted to the computer center (authentication center AC), whereafter the card is issued to the sales organization. The AC therefore has already stored all subscriber identification numbers IMSI and the associated secret keys Ki at the time the respective card is issued and has to administer these identification numbers and keys, although the respective card has not yet been sold and is still in the possession of the vendor. Consequently, cards which have not yet been sold are stored in large numbers of sales offices, while the data of these cards have to be administered by the AC.

In addition, it may happen that when a manufacturer or another member of the sales organization attempts to personalize the cards, the key may have already be compromised. The initial personalization of the chip is therefore not secure and may be subject to misuse.

EP-A-562 890 discloses a mobile communication network having the capability for remotely updating a so-called subscriber identification module (SIM) in mobile stations. The SIM stores data for controlling the mobile stations and for access to the services of the mobile radio network. The data stored in the SIM can be changed, i.e., updated, over the radio air interface. However, a method for personalizing a SIM over the air interface is not described.

Replacement sheet 2a

WO-A-97/14258 also describes a method and a device for programming a mobile station via an air interface. Optionally, programs stored in the mobile station are here replaced or additional data are transmitted via the air interface. The method described herein also permits an initial activation of the mobile station via the air interface, but not a personalization of a subscriber identification module.

WO-A-93/07697 relates to a method for personalizing an active so-called SIM card. The SIM card is here completely personalized in an authorized terminal equipment which is connected via an encrypted communication line with a the central computer of the mobile radio network. However, a personalization of the chip card when the subscriber first logs on to the mobile radio network, is also neither taught nor suggested by this reference.

It is therefore an object of the invention to improve a method, a device and a chip of the aforedescribed type so that the overly complex administration in the AC can be simplified and the secret data of the chip can be stored more securely.

To solve the object, the invention is characterized by the technical teachings of claim 1. A chip according to the invention is characterized by the technical teachings of claim 6.

Replacement sheet 3:

The technical teachings according to the invention attains the following advantages:

Elimination of a central personalization at the network operator
Issuance of a large number of GSM chips without producing a static load at the network operator
Reuse of "used" GSM chips
Regular change of the secret key Ki while used by the customer.

With the proposed method, the device manufacturer/chip manufacturer applies initial data associated with the card to the chip, which could be referred to as pre-personalization. The network operator himself performs the actual personalization at a later time and only for those customers who enter into a contract with the network operator.

The pre-personalization does not yet produce a static load at the network operator. The method therefore makes it possible to distribute "millions" of GSM chips, for example in each and every automobile, in each laptop computer or in each alarm system, and to subsequently "activate" only the chips of those customers who enter into a contract.

It is also possible to reuse cards if a customer terminates his contract (for example, if he sells his automobile).

In particular, in the case of the network operator D1, the dealer could release returned cards again for another customer. The network operator therefore eliminates the personalization of cards in the terminal equipment replacement business.

To implement the technical teachings, the GSM chip can advantageously be Toolkit-enabled. In particular, the terminal equipment should be able to transmit short messages to the network operator. The chip should also offer a function to restore the initial state of the chip (see below).

The terminal equipment or a different device may also use this function of the chip. The terminal equipment should also be able to read the card number and the version number (see below). (Alternatively, the card number and the version number could be indicated on the GSM card).

The chip manufacturer is responsible for the pre-personalization. ICCID and IMSI are taken from a pool of numbers, whereas the chip itself derives from a key K1 which is known to the chip manufacturer, an initial key Ki_1. PIN and PUK are set to a default value.

No entry is made into the AC

When a customer is signed up, an entry is made in the AC. This entry is also derived from the initial key Ki_1.

The hotlining flag is set in the HLR

The first call is routed to a security center

The security center negotiates a new Ki_2 as well as a PUK, using the Diffie-Hellman method.

Used chips intended for reuse are reset with an internal function.

Pre-personalization at the chip manufacturer is carried out by allocating a range of card numbers and subscriber identification numbers to each chip manufacturer. The number ranges for ICCID and IMSI are large enough to make this possible.

The chip manufacturer also receives the following data from the network operator: a, p, VER, K1.

The chip manufacturer then applies the following data to each chip:

ICCID card number

IMSI subscriber identification number (is tied to ICCID, for example, by having the same position within the two number ranges for ICCID and IMSI)

a a sufficiently large number forming the basis for Diffie-Hellman

p a sufficiently large number, prime number for Diffie-Hellman

VER a version number, for example 8 bytes, unique for each chip manufacturer (can be changed from time to time)

K1 8 bytes DES key, uniquely tied to VER.

Note: The network operator could derive the key K1 from the version number VER using a master key (for example with the DES method). However, this is not required.

The chip then generates the following secret numbers:

Ki_1 Ki_1 is an initial Ki which the chip derives from the IMSI using the DES key K1.

PIN PIN is set to a fixed value of 0000.

PUK PUK is set to a fixed value of 00000000.

Optionally, additional secret numbers.

The chip must retain K1 and the generated secret numbers in a secure region and protect these numbers from being read.

The processes in the authentication center AC:

The AC knows the key K1 of each version number VER (K1 can be derived from VER using a master key so that the values K1 issued to the chip manufacturer do not need to be stored).

The initial values Ki_1 generated by the chips are not recorded in the AC.

Since the AC does not yet know the IMSI's, no static load is produced.

Customer sign-up and release by the network operator

A customer who wishes to use his device (his card, his chip), enters into a contract with the network operator. The card number (ICCID) identifies the chip.

The network operator activates the following actions:

Reading or obtaining the card number and version number (ICCID, VER)

The IMSI is permanently associated with the ICCID

IMSI and VER are entered into the AC (it is only now that the subscriber relationship is made known in the AC)

The AC knows the key K1 which is permanently tied to VER and generates from K1 the initial key Ki_1 from the IMSI, using the same method being used in the chip

- The HLR sets the "hotlining flag" to this IMSI. The first call is then routed to an SC (security center). (The SC could also be the HLR/AC itself)

The first call: final personalization of the chip

Since the chip and the AC now have knowledge of the same secret key Ki_1, the chip logs on to the network. (The PIN is 0000 and known to the customer)

With hotlining enabled, the first call is automatically routed to the SC. Depending on the software in the Toolkit-enabled terminal equipment, the first call could already be a short message

The SC advantageously uses the Toolkit-features of the chip and negotiates with the chip a new secret key Ki_2.

The Diffie-Hellman method is used herein which has the following advantages:

Keys of arbitrary length can be negotiated

It is not sufficient to listen to the air interface to extract the generated key.

The chip stores the new key Ki_2 (this key is subsequently used for authentication).

- The new key can be immediately verified (for example, challenge response, as is customary with GSM);
- The SC transmits the new key Ki_2 to the AC;
- By again using Diffie-Hellman, the SC negotiates a PUK (or additional secret numbers) with the chip. (The network operator can subsequently communicate the secret numbers to the customer or retain the secret numbers for service purposes)
- The hotlining flag in the HLR is removed. Normal calls are now enabled, with the new secret key Ki_2 being used from this time on;
- The Toolkit-enabled terminal equipment informs the customer about success or failure;
- The Toolkit-enabled terminal equipment may aks the customer to select a new PIN.

<u>Reuse of used chips/cards</u>

It will be assumed that the subscriber relationship is removed from the HLR and the AC because the customer has terminated his contract. When a contract is entered with the new customer and a used chip is reused, the following steps are executed:

First, the function of the terminal equipment to initialize the chip is employed.

Thereafter, in the chip:

Ki_2 is deleted

Ki_1 is reactivated

The PIN is set to 0000

The PUK is set to 00000000 (in an analogous manner, with additional secret numbers PUK2)

This function could, for example, be activated within the D1 network by the X13 which is installed at many dealer sites. In this way, the dealer can issue another initialized card.

The additional steps are identical to those for customer sign-up and release by the network operator (see above).

Change of the secret key during the utilization time of the chip

The network operator can force a change of Ki in regular intervals. This can be done simply by enabling the hotlining flag in the HLR which routes the call to the SC and, as described above, by negotiating a new Ki. However, the PUK should not be renegotiated at this time.

Possibilities for misuse (illustrated here for D1)

1. The key K1 of a chip manufacturer is compromised and a card is copied.

1.1 The IMSI is not yet known in the AC. The card does not register.

1.2 The IMSI of the genuine card is already in the AC and has already been provided with the final personalization.
The forged card cannot log on since Ki_1 is different from Ki_2 (authentication failed).

1.3 The genuine IMSI is already in the AC, but final personalization has not yet been performed.
This refers to the brief time interval between the time the contract takes effect and the device is switched on for the first time. During this time interval, a forged card could be "inserted." The genuine card would then not be able to log on because it does not have the Ki_2 of the forged card. This scenario could be prevented, for example,

by including - at the time of the subscription - on the order document a secret number which the customer has to provide after receiving the key. This secret number is sent to the SC where it is checked.

2. The customer initializes his own card (for example with X13). Thereafter, the card has the key Ki_1 and does no longer log on.

The invention will now be described with reference to an embodiment illustrated in the drawings. Additional features and advantages are disclosed in the drawings and in the description of the drawings.

It is shown in:

Figure 1: schematically, the pre-personalization of the cards at the chip manufacturer;

Figure 2: schematically, the processes during the release by the network operator (final personalization);

Figure 3: schematically, the processes when the chip is erased and reused.

Figure 1 illustrates in the form of a drawing what has already been described on page 4 of the description, namely that the card number ICCID is provided in a range between a number X and a number Y.

The same applies to the subscriber identification number IMSI which is also located in a range of values between A and B.

In the two number ranges allocated for ICCID and IMSI, a number a is selected as a base for the Diffie-Hellman algorithm as well as a number p which serves as a prime number for the Diffie-Hellman encryption.

Also defined is a number VER which can be a functional number having a length of 8 bytes. In addition, the key X1 is computed in form of a DES key which is tied to VER.

The aforedescribed data are entered into the card, with the chip generating (computing) the secret number Ki_1 which is stored in the card. The card is supplied in this form (pre-personalized) to the VO (sales organization).

Figure 2 illustrates the individual processes which are described in the description starting on page 5 .

In a first process step, the VO enters into a contract with the customer. In the same process step, the card number ICCID and the version number together with the contract are entered in an order confirmation, wherein this order confirmation is communicated in a second process step to the AC together with the subscriber identification number and the version number VER.

At the same time, the subscriber identification number IMSI is communicated to the HLR so that the HLR is made aware of the card data and establishes the so-called hotlining flag.

The customer now receives his pre-personalized card and establishes in a first call - which according to the present invention is forcibly switched to the SC - contact with the SC. In this first call, the Ki_2 is negotiated as well as the PUK, with the new PIN being set at the same time. At the same time, the SC verifies the secret key Ki_2 with respect to the card.

In a fourth method step, the SC contacts the HLR and removes the hotlining flag, which in turn enables the customer to make unrestricted calls.

Replacement sheet 11:

In the fourth method step, the SC also communicates the secret key Ki_2 to the AC.

At this point, the card is released and provided with the final personalization.

The reuse of used cards has been described in detail above. As seen from Fig. 3, the customer contacts with his card the VO which enters the card number ICCID into the order confirmation so that the IMSI is deleted both in the AC and in the HLR.

In this way, the key Ki_2 is deleted and the key Ki_1 is reactivated and stored in the card. Likewise, the PIN is set to the value 0000 and also the PUK.

The card, having been pre-personalized in this way, can now be sent to a card pool and reissued to new customers.

In other words, the final personalization is reversed so that the card is in the same state as when it was pre-personalized.

It should also be noted that the network operator where the order is placed, is also referred to as Order Receiving Office and that this Order Receiving Office has knowledge of the association between ICCID and IMSI due to their 1:1 association within the issued range of numbers.

Claims

1. Method for personalizing GSM chips having a memory range in which at least one subscriber identification number IMSI and a card number ICCID are stored, and wherein for personalizing the chip an additional secret key Ki and, optionally, additional data are stored,
characterized in that the chip is personalized at the time when the subscriber logs on to the subscriber network.

2. The method according to claim 1, characterized in that the chip is personalized when the subscriber logs on to the subscriber network for the first time.

3. The method according to claim 1 or 2, characterized in that for pre-personalizing the chip at the manufacturer, at least initial, card-specific data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK are stored.

4. The method according to one of the claims 1-3, characterized by the following process steps:

in a first process step, the chip manufacturer obtains the ICCID and the IMSI from a number pool, the chip itself derives an initial key Ki_1 from a key K1 which is known to and entered into the chip by the chip manufacturer, while PIN and PUK are set to a default value,

in a second process step, an entry is made in the AC and HLR as soon as a subscriber has entered into a contract with the network operator,

in a third process step, the AC also derives the initial first key Ki_1,

in a fourth process step, the network sets the conditions so that during logon to the network, a connection is established from the chip to the component SC (security center of the network operator),

in a fifth process step, the connection is routed from the chip to the SC during the first logon,

in a sixth process step, a new, second secret key Ki_2 and, optionally, a PUK is negotiated with the chip (for example using the Diffie-Hellman method) or generated in the SC and transmitted to the chip, in a seventh process step, the conditions of the fourth process step are disabled again.

5. The method according to one of the claims 1-4, characterized in that the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established.

6. Chip for carrying out the method according to one of the claims 1-5, characterized in that the chip in the terminal equipment is Toolkit-enabled and can communicate with the SC and negotiate a key.

7. The chip according to claim 6, characterized in that the chip can receive data from the SC and writes these data to its memory and, optionally, reads these data from the memory the and changes the data and/or transmits the data to the computer center (SC).

8. The chip according to one of the claims 6 or 7, characterized in that the micro-processor of the chip negotiates a secret key with the SC.

9. The chip according to claim 8, characterized in that the key of the method is negotiated using the Diffie-Hellman method.

10. The chip according to one of the claims 6-9, characterized in that the chip has a dialing number which is fixedly pre-programmed by the manufacturer (fixed dialing).

11. Computer center for carrying out the method according to one of the claims 1-5, characterized in that the HLR is capable of setting and deleting a rerouting command (hotlining flag).

12. Computer center for carrying out the method according to one of the claims 1-5, by using a chip according to one of the claims 6-10, characterized in that the network sets conditions so that a connection is established from the chip to the component SC during logon to the network.

13. Computer center for carrying out the method according to one of the claims 1-5, by using a chip according to one of the claims 6-10, characterized in that the hotlining flag is set in the HLR when the initial key Ki_1 is a first entered in the AC.

SUMMARY

The invention relates to a method for personalization of GSM chips. At least one subscriber identification character (TMSI) and a card number (ICCID) are stored in the memory area of said chips in addition to a secret key (KI) and other optional data for personalization purposes. The invention aims to eliminate an unnecessarily high degree of complexity linked to management of all card data in an authentication centre (AC) and to preserve secret chip data in a more secure manner. According to the invention, final data is only written on the chip when the subscriber logs into a subscriber network. One advantage is that only initial data is written into the card enabling the customer to contact the computer centre of the information provider. During first contact the final data is traded between the card and the computer centre and written into the card. The computer centre is simply required to manage cards which have really been issued to customers.

09/485352

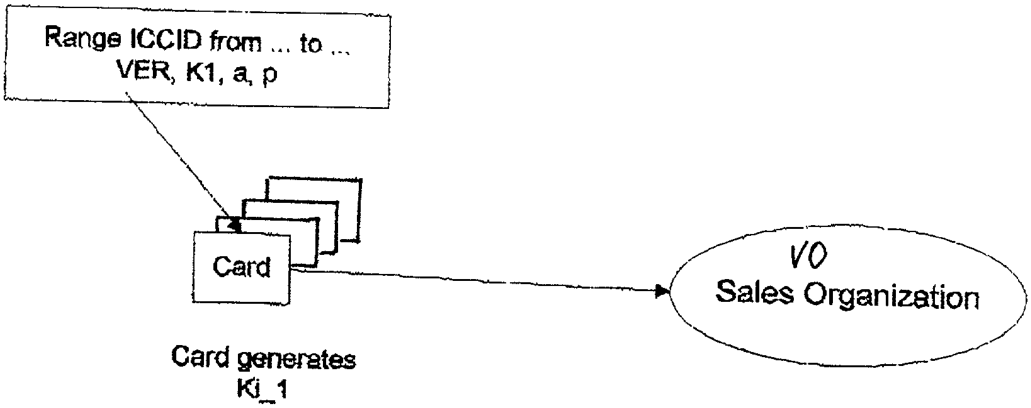

FIG. 1

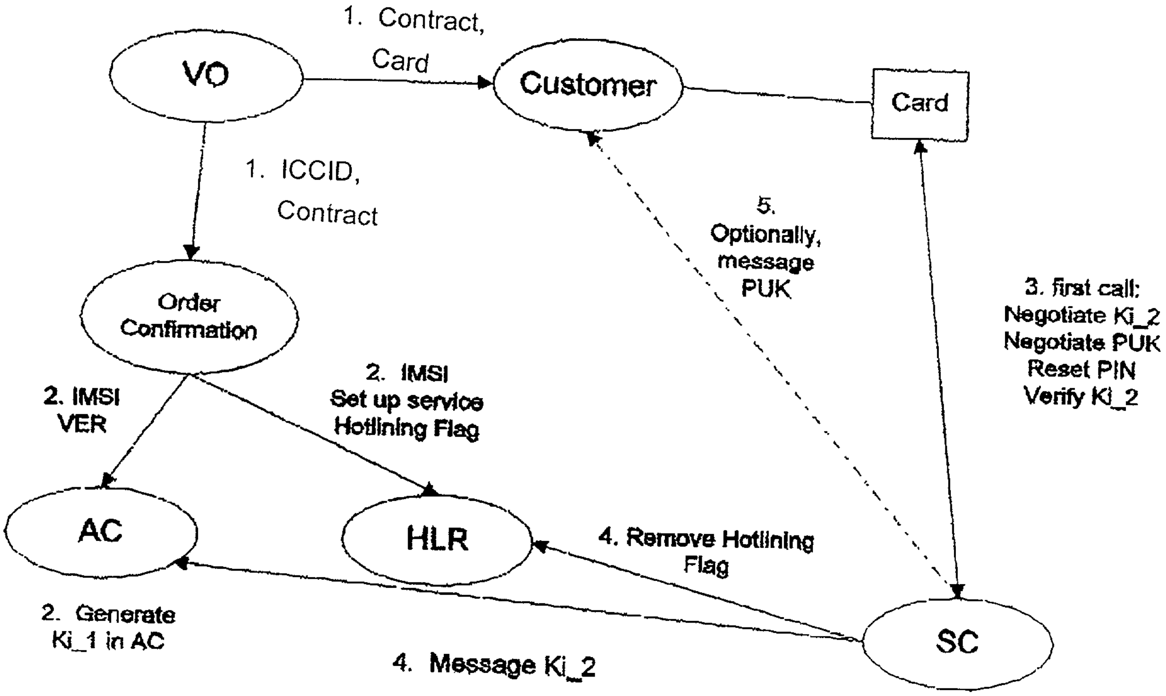

FIG. 2

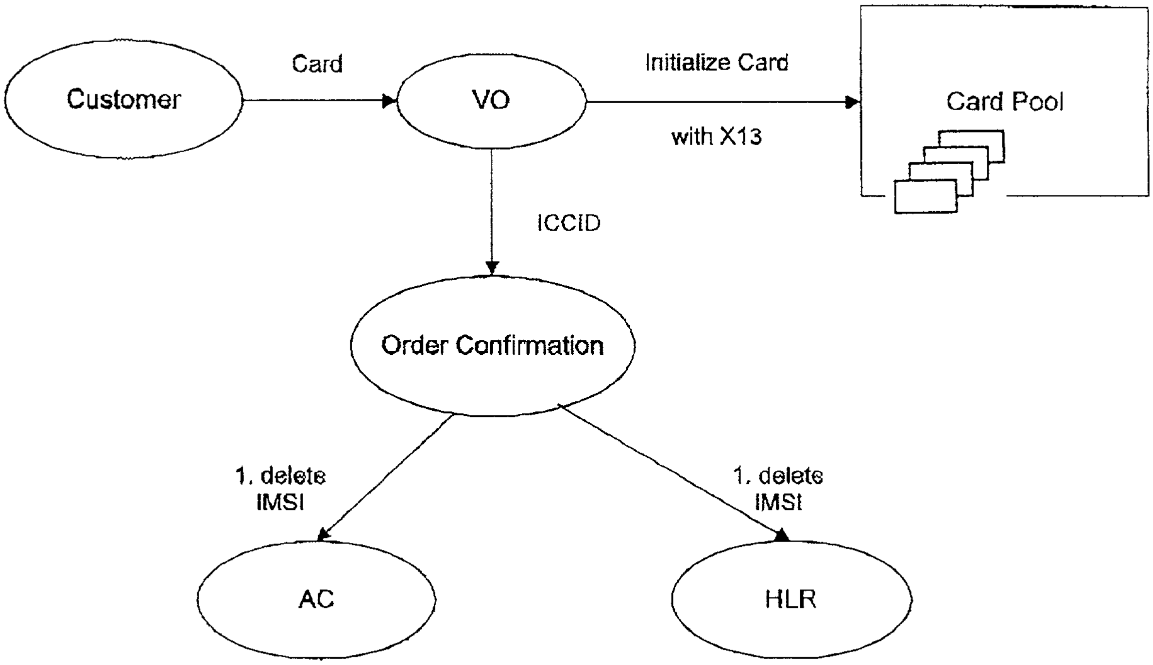
Customer
Card
VO
Initialize Card
with X13
Card Pool
ICCID
Order Confirmation
1. delete IMSI
1. delete IMSI
AC
HLR

FIG. 3

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

(Includes Reference to PCT International Applications)

ATTORNEY DOCKET NUMBER
2643/0G629

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed for and which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR CUSTOMER PERSONALIZATION OF GSM CHIPS
the specification of which (check only one item below):

[ ] is attached hereto.

[ ] was filed as United States application

Serial No. __________

on _______

and was amended

on _______ (if applicable).

[X] was filed as PCT international application

Number PCT/DE98/01943

on July 13, 1998

and was amended under PCT Article 19

on _______ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

COUNTRY (if PCT indicate PCT)	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C 119
PCT	PCT/DE98/01943	13 July 1998	[] YES [X] NO
GERMAN	197 33662.0	4 August 1997	[X] YES [ ] NO
			[ ] YES [] NO
			[ ] YES [ ] NO

Combined Declaration for Patent Application and Power of Attorney (Continued) (Includes Reference to PCT International Applications)	ATTY'S DOCKET NUMBER **2643/0G629**

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S APPLICATIONS			**STATUS (Check one)**		
U.S APPLICATION NUMBER		U.S. FILING DATE	PATENTED	PENDING	ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.					
PCT APPLICATION NO	PCT FILING DATE	U S SERIAL NUMBER ASSIGNED (if any)			

18

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. Gordon D. Coplein #19,165, William F. Dudine, Jr. #20,569, Michael J. Sweedler #19,937, S. Peter Ludwig #25,351, Paul Fields #20,298, Joseph B. Lerch #26,936, Melvin C. Garner #26,272, Ethan Horwitz #27,646, Beverly B. Goodwin #28,417, Adda C. Gogoris #29,714, Martin E. Goldstein #20,869, Bert J. Lewen 19,407, Henry Sternberg #22,408, Peter C. Schechter #31,662, Robert Schaffer #31,194, Robert C. Sullivan, Jr. #30,499, and Joseph R. Robinson #33,448, Chista Hildebrand #34,953

Send Correspondence to:

Christa Hildebrand, Esq.
DARBY & DARBY P.C.
805 Third Avenue
New York, New York 10022-7513

Direct Telephone Calls to:
(name and telephone number)

(212) 527-7700

2	FULL NAME OF INVENTOR	FAMILY NAME DUPRÉ	FIRST GIVEN NAME Michael	SECOND GIVEN NAME
0	RESIDENCE & CITIZENSHIP	CITY SANKT AUGUSTIN DEX	STATE OR FOREIGN COUNTRY GERMANY	COUNTRY OF CITIZENSHIP GERMAN
1	POST OFFICE ADDRESS	POST OFFICE ADDRESS ZEDERNWEG 175	CITY D-53757SANKT AUGUSTIN	STATE & ZIP CODE/COUNTRY GERMANY
2	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
0	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
2	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
2	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
0	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
3	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

SIGNATURE OF INVENTOR 201 Dupré	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
DATE 21.2.2000	DATE	DATE